UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ELIANA EPSTEIN, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. ENZO BIOCHEM, INC., ENZO CLINICAL LABS, INC., and LAB CORPORATION OF AMERICA HOLDINGS, Defendant.	**CASE NO. 23-4282** **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff ELIANA EPSTEIN ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants ENZO BIOCHEM, INC., ENZO CLINICAL LABS, INC., and LAB CORPORATION OF AMERICA HOLDINGS ("Enzo Biochem", "Enzo Clinical", and "Labcorp" or, collectively, "Defendants") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Enzo Biochem, Enzo Clinical, and Labcorp (the "Data Breach").

2. Defendants' breach differs from typical data breaches because it affects consumers who had no relationship with Defendants, never sought one, and never consented to Defendants collecting and storing their information.

3. Enzo Clinical sourced their information from third parties, stored it on Defendants' systems, and assumed a duty to protect it, advertising that Defendants "respect[] individual privacy and values the confidence of its customers, partners, investors and employees."[1] But Defendants never implemented the security safeguards needed despite acknowledging its importance.

4. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names, Social Security numbers, dates of service, ("personal identifying information" or "PII"), and clinical test information ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

5. On information and belief, the Data Breach occurred between April 4, 2023, and April 6, 2023. Defendants did not become aware of suspicious activity on its network until April 6, 2023, allowing cybercriminals unfettered access to Plaintiff's and the Class's highly private Sensitive Information for two days.

6. On May 31, 2023, Defendants began notifying Plaintiff and Class Members about the widespread Data Breach ("Notice Letter"), with Plaintiff's Notice Letter attached as Exhibit A. Defendants waited almost two months before informing Class Members even though Plaintiff and approximately 2.5 million Class Members had their most sensitive personal information accessed, exfiltrated, and stolen,[2] causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

[1] Privacy Policy, Enzo, https://enzo.com/footer-links/privacy-policy (last visited June, 9, 2023).
[2]Clinical test data of 2.5 million people stolen, DataBreaches.net https://www.databreaches.net/clinical-test-data-of-2-5-million-people-stolen-from-biotech-company-enzo-biochem/ (last visited June, 9, 2023).

7. Defendants Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened, or why it took Defendants nearly two months to begin notifying victims that hackers had gained access to highly private Sensitive Information.

8. Defendants' failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

9. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

10. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed an unknown number of their consumers.

11. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their Sensitive Information. But Defendants betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff Eliana Epstein is a Data Breach victim.

13. The exposure of one's Sensitive Information to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

14. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together

with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

PARTIES

15. Plaintiff, Eliana Epstein, is a natural person and citizen of Massachusetts, residing in Boston, Massachusetts, where she intends to remain. Plaintiff Epstein is a Data Breach victim, receiving the Breach Notice on June 8, 2023.

16. Defendant Enzo Biochem is a New York Corporation, with its principal place of business at 81 Executive Blvd. Suite 3, Farmingdale, NY, United States, 11735.

17. Defendant Enzo Clinical, is a New York Corporation, with its principal place of business at 28 Liberty Street, New York, NY, United States, 10005.

18. Defendant Labcorp is a North Carolina Corporation, with its principal place of business at 531 South Spring Street, Burlington, NC, United States, 27215.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Plaintiff and Defendants are citizens of different states.

20. This Court has personal jurisdiction over Defendant Enzo Biotech because Defendant maintains its principal place of business in this District and does substantial business in this District.

21. This Court has personal jurisdiction over Defendant Enzo Clinical because Defendant maintains its principal place of business in this District and does substantial business in this District.

22. This Court has personal jurisdiction over Defendant Lapcorp because Defendant does substantial business in this District.

23. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Enzo Biotech and Enzo Clinical Labs

24. Defendants proclaim themselves as "pioneer['s] in molecular diagnostics", touting their position "as a global company", "leading the convergence of clinical laboratories, life sciences, and intellectual property' with their "technology [targeting] specific market needs".[3]

25. As part of their business, Defendants receive and maintain the Sensitive Information of thousands of consumers. In doing so, Defendants implicitly promise to safeguard their Sensitive Information.

26. Indeed, Defendants promise in their Privacy Policy that they "respect [] individual privacy and values the confidence of its customers, partners, investors and employees".[4]

27. Defendants additionally assure their consumers that the data they collect "will not be transferred outside the company without your prior consent" and that Defendants "will make [] every reasonable effort to protect the information collected".[5]

[3] About us, Enzo, https://www.enzo.com/#:~:text=Enzo%20Biochem%20is%20a%20pioneer,numerous%20advantages%20over%20previous%20standards (last visited June 9, 2023).
[4] Privacy Policy, Enzo, https://enzo.com/footer-links/privacy-policy (last visited June, 9, 2023).
[5] *Id.*

28. With the PHI they collect, Defendants recognizes that they "understand that your medical information is private and confidential. Further, we are required by law to maintain the privacy of protected health information.[6]

29. As Plaintiff alleges above, Defendants collect data on individuals who have no relationship with it, do not want one, and have never consented to their services.

30. They do so by sourcing that information from third parties.

31. In collecting and maintaining consumers' Sensitive Information, Defendants agree that they would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information

32. Despite recognizing their duty to do so, on information and belief, Defendants have not implemented reasonably cybersecurity safeguards or policies to protect their consumers' Sensitive Information or supervised their IT or data security agents and employees to prevent, detect, and stop breaches of their systems. As a result, Defendants leaves significant vulnerabilities in their systems for cybercriminals to exploit and gain access to consumers' Sensitive Information.

Labcorp

33. Labcorp touts itself as "a leading global life sciences company" who's mission is "to improve health and improve lives" by delivering "world-class diagnostic solutions, [and] innovative medicines to patients faster and uses technology to improve the delivery of care." [7]

[6] *Id*.
[7] Company Information, Labcorp, https://www.labcorp.com/frequently-asked-questions/patient/general/company-information#:~:text=Labcorp%20is%20a%20leading%20global,improve%20the%20delivery%20of%20care (last visited June 9, 2023).

34. On information and belief, Labcorp purchased Enzo Clinical on March 17, 2023. [8]

35. As part of its business, Defendant receives and maintains the Sensitive Information of thousands of consumers. In doing so, Defendant implicitly promises to safeguard their Sensitive Information.

36. As Plaintiff alleges above, Defendant collects data on individuals who have no relationship with it, do not want one, and have never consented to its services.

37. It does so by sourcing that information from third parties.

38. In collecting and maintaining consumers' Sensitive Information, Defendant agrees that it would safeguard the data in accordance with state and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information

39. Despite recognizing their duty to do so, on information and belief, Defendants have not implemented reasonably cybersecurity safeguards or policies to protect their consumers' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendants leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Sensitive Information.

The Data Breach

40. On information and belief, Defendants collect and maintain consumers' Sensitive Information in its computer systems.

41. In collecting and maintaining Sensitive Information, Defendants implicitly agree that they will safeguard the data using reasonable means according to their internal policies, as well as state and federal law.

[8] MedCity News, https://medcitynews.com/2023/03/labcorp-shells-out-146m-to-buy-enzo-biochems-clinical-lab-business/ (last visited June 9, 2023).

42. According to the Breach Notice, on April 6, 2023, Defendants "identified a ransomware incident on [its] computer network," and that "[an] investigation determined that an unauthorized party accessed files on our systems between April 4, 2023, and April 6, 2023." Ex. A.

43. In other words, Defendants' investigation revealed that their cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly private Sensitive Information.

44. On or around May 31, 2023 –almost two months after the Breach first occurred– Defendants finally began notifying Plaintiff and Class Members about the Data Breach.

45. Despite their duties and alleged commitments to safeguard Sensitive Information as "leaders" within their industry, Defendants did not in fact follow industry standard practices in securing consumers' Sensitive Information, as evidenced by the Data Breach.

46. In response to the Data Breach, Defendants contend that they have or will "take steps to enhance the security of our computer systems and data we maintain". Ex. A. Although Defendants fails to expand on what these alleged "steps" are, such steps should have been in place before the Data Breach.

47. Through their Breach Notice, Defendants recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to remain "vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity." Ex. A.

48. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach

and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

49. On information and belief, Defendants has offered two years complimentary credit monitoring and identity monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

50. Even with two years' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

51. On information and belief, Defendants failed to adequately train and supervise their IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over their consumers' Sensitive Information. Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

52. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and healthcare adjacent industry preceding the date of the breach.

53. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendants knew or should have known that their electronic records and consumers' Sensitive Information would be targeted by cybercriminals.

54. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[10]

55. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[11]

56. Cyberattacks on medical systems and healthcare partner and provider companies like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12]

57. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendants.

---

[9] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).
[10] *Id.*
[11] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).
[12] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

Plaintiff Epstein's Experience

58. Plaintiff Epstein was injured by Defendants' Data Breach.

59. Plaintiff is unsure how Defendants got her information, but assumes a healthcare provider she received treatment from provided Defendants with her Sensitive Information.

60. Despite never forming or seeking a relationship with Defendants, Plaintiff's Sensitive Information, including her name, Social Security Number, date of service, and clinical test information, was compromised in Defendants' Data Breach, exposing her to identity theft and fraud.

61. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for two months.

62. Plaintiff does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

63. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

64. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

65. Plaintiff has and is experiencing feelings of anxiety, sstress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience;

it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

66. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Defendants were required to adequately protect.

67. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

68. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

69. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendants.

70. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

71. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

72. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

73. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

74. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

75. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

76. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

77. Defendants disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

78. Defendants' failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest

ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants failed to adhere to FTC guidelines.

79. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of Sensitive Information.

80. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

81. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

82. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

85. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [13]

86. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[14]

[13] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[14] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

87. The Data Breach itself resulted from a combination of inadequacies showing Defendants' failure to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that they create, receive, maintain and transmit in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents

that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

88. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants Failed to Comply with Industry Standards

89. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

90. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

92. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

93. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

94. Plaintiff sues on behalf of herself and the proposed nationwide class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class**: All individuals residing in the United States whose Sensitive Information was compromised in the Defendants' Data Breach including all those who received notice of the breach.

95. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants'

officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

96. Plaintiff reserves the right to amend the class definition.

97. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at least 2.5 million members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

98. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

99. Plaintiff realleges all previous paragraphs as if fully set forth below.

100. Plaintiff and members of the Class entrusted their Sensitive Information to Defendants. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in

handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

101. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

102. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

103. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants'

inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's Sensitive Information.

104. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Sensitive Information —whether by malware or otherwise.

105. Sensitive Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

106. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

107. Defendants' breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their

Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

108. Plaintiff realleges all previous paragraphs as if fully set forth below.

109. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

110. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's Sensitive Information.

111. Defendants breached their duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

112. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their consumers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common

law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

113. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

114. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

115. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

116. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

117. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

118. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

119. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

120. Had Plaintiff and the Class known that Defendants did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendants with their Sensitive Information.

121. Defendants' various violations and their failure to comply with applicable laws and regulations constitute negligence *per se*.

122. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information;

and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

123. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

COUNT III
Breach of Contract
(On Behalf of Plaintiff and the Class)

124. Plaintiff realleges all previous paragraphs as if fully set forth below.

125. Defendants entered into various contracts with its clients, including healthcare providers, to provide software services to its clients.

126. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential medical information that Defendants agreed to collect and protect through their services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

127. Defendants knew that if they were to breach these contracts with their healthcare provider clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Sensitive Information.

128. Defendants breached their contracts with their clients when they failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Sensitive Information.

129. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendants failure to use reasonable data security measures to store their Sensitive Information, including but not limited to, the actual harm through the loss of their Sensitive Information to cybercriminals.

130. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

131. Plaintiff realleges all previous paragraphs as if fully set forth below.

132. Plaintiff and members of the Class conferred a benefit upon Defendants in providing Sensitive Information to Defendants.

133. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the services and goods they sold to their consumers, including Plaintiff's and the Class.

134. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class's Sensitive Information because Defendants failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendants had they known Defendants would not adequately protect their Sensitive Information.

135. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Violation Of The New York Deceptive Trade Practices Act ("GBL")
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff and the Class)

136. Plaintiff realleges all previous paragraphs as if fully set forth below.

137. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Sensitive Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of their privacy and security protections for Class Members' Sensitive Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

138. Defendants knew or should have known that their network and data security practices were inadequate to safeguard the Class Members' Sensitive Information entrusted to it, and that the risk of a data breach or theft was highly likely.

139. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

140. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendants' network and aggregation of Sensitive Information.

141. The representations upon which consumers (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendants' adequate protection of Sensitive Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

142. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

143. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Sensitive Information and that the risk of a data security incident was high.

144. Defendants' acts, practices, and omissions were done in the course of Defendants' business of furnishing employment benefit services to consumers in the State of New York. 167.

145. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Sensitive Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

146. As a direct and proximate result of Defendants' multiple, separate violations of GBL §349, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in

the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

147. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

148. Plaintiff brings this action on behalf of herself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendants' unfair, deceptive, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

149. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

150. On behalf of herself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover her actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

151. Also as a direct result of Defendants' violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: June 9, 2023

Respectfully submitted,

By: /s/ James J. Bilsborrow

James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, New York 10003
Telephone: (212) 558-5500
jbilsborrow@weitzlux.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class